AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A system for providing network-based firewall policy configuration and facilitation associated with a firewall, the system comprising:

a firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy, and to generate a time window during which a user can run the application; and

a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured:

to receive a firewall modification request from the firewall facilitation coordinator,

to ~~be aware of communications or packets observed by the firewall during the time window,~~ determine whether the application includes one or more questionable packets, and

to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.

2. (Currently Amended) The system of claim 1, further ~~comprises~~ comprising a firewall process adapted to communicate with the policy modification agent, the firewall process ~~includes~~ including the user's firewall policy, a firewall ~~communications or~~ packet inspector and a firewall filter.

3. (Currently Amended) The system of ~~claim 2~~ claim 1, wherein the firewall facilitation coordinator is further configured to decode and decrypt the firewall modification request, and further configured to authenticate the user before taking action on the request.

4. (Currently Amended) The system of ~~claim 3~~ claim 1, wherein the firewall facilitation coordinate further comprises at least one of a secure transceiver, a firewall facilitation

coordinator controller, a user notification authenticator, a user database, or a firewall policy configuration/modification window generator.

5. (Currently Amended) The system of ~~claim 4~~ claim 1, wherein the policy modification agent further comprises at least one of a secure transceiver, policy modification agent controller, policy modifier, blocking history checker or blocking database.

6. (Currently Amended) ~~The system of claim 5, wherein the user exercises the application during the time window with that application transmitting/receiving packets through the network-based firewall with communications or packets associated with the application passing through the network-base firewall unblocked~~ The system of claim 1, wherein the policy modification agent is further configured to determine whether the firewall modification request is associated with a first attempt to modify the user's firewall policy, and wherein if the application is determined to include one or more questionable packets and the firewall modification request is associated with a first attempt, the at least a portion of the packets associated with the application does not include the one or more questionable packets.

7. (Currently Amended) ~~The system of claim 5, wherein during the time window, the policy modification agent via the firewall process examines communications or packets associated with the application and modifies the user's firewall policy such that the communications or packets are allowed to pass through the firewall process unblocked~~ The system of claim 6, wherein if the application is determined to include one or more questionable packets and the firewall modification request is not associated with a first attempt, the at least a portion of the packets associated with the application includes at least a portion of the one or more questionable packets.

8. (Currently Amended) The system of claim 1, ~~further comprises a blocking history checker for checking communications or packets observed during the time window to be associated with the application in order to identify~~ wherein the one or more questionable ~~communications or~~ packets ~~which are defined as those communications/packets~~ include packets or ~~communications/packet~~ packet types that are already part of the user's firewall policy or

~~communications or~~ packets previously blocked at times other than during the time window but which are now observed during the time window.

9. (Canceled)

10. (Currently Amended) The system of ~~claim 9~~ claim 1, wherein if the application is determined to include one or more questionable packets, the policy modification agent is further configured to record the one or more questionable ~~communications or packet types~~ packets in a blocking history database.

11. (Currently Amended) The system of ~~claim 10~~ claim 1, wherein the policy modification agent is further configured to send an acknowledgement ~~of questionable communications or packet types recorded in the blocking history database~~ to the user via the firewall facilitation coordinator that modification of the user's firewall policy was successful, the acknowledgement including an alert regarding the one or more questionable packets if the application is determined to include the one or more questionable packets.

12. (Currently Amended) The system of ~~claim 10~~ claim 1, wherein the policy modification agent is further configured to attempt to modify the user's firewall policy a configurable number of times; and if unsuccessful, to notify the user~~/customer~~ to seek assistance or to notify appropriate personnel for assistance.

13. (Currently Amended) The system of ~~claim 8~~ claim 1, wherein if the application is determined to include one or more questionable packet, the policy modification agent is further configured to group the ~~types of~~ one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets ~~singly and in combinations of two or more~~.

14. (Currently Amended) The system of claim 13, wherein the policy modification agent is further configured to prioritize the groups based on a likelihood that the groups will be

required to be added to the user's firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

15. (Currently Amended) The system of ~~claim 13~~ claim 14, wherein the policy modification agent is further configured to perform successive policy modification attempts to remove ~~previously added~~ one or more of the questionable packet groups previously included in the portion of the packets associated with the application and to add one or more of the questionable packet groups having ~~the~~ a next highest priority ~~group~~ to the ~~firewall policy~~ the portion of the packets associated with the application.

16. (Currently Amended) A method for modifying a firewall policy of a network-based firewall, the method comprising:

~~notifying a coordinating entity of~~ receiving a request to modify the firewall policy to incorporate filtering rules to allow ~~communications or~~ packets associated with ~~from~~ a new application to pass through the network-based firewall without being blocked;

~~notifying a policy modifier of the modification request;~~

sending a user an indication of a time ~~period~~ window during which the user can exercise ~~a new~~ the new application; ~~and~~

examining the ~~communications or~~ packets traversing to/from the network-based firewall from/to the user to determine whether the new application includes one or more questionable packets; and

modifying the ~~user's~~ firewall policy ~~such that necessary communications or packets associated with the new application are allowed~~ to allow at least a portion of the packets associated with the new application to pass through the network-based firewall unblocked, the at least a portion of the packets associated with the new application determined based on whether the new application includes one or more questionable packets.

17. (Original) The method of claim 16, further comprising acknowledging the modification request and sending an acknowledgement of the modification request to a user's processing device.

18. (Original) The method of claim 16, further comprising authenticating the user before acting on the modification request.

19. (Currently Amended) The method of claim 16, ~~wherein~~ further comprising notifying ~~a coordinating entity and~~ a policy modifier of ~~a request~~ the request to modify ~~a firewall~~ the firewall policy, ~~step~~ wherein notifying the policy modifier further comprises providing a name of the new application and a time frame for ~~implementation of configuration change~~ modifying the firewall policy.

20. (Currently Amended) The method of claim 16, further comprising sending an acknowledgement of completion of the modification to ~~the~~ a user's processing device.

21. (Currently Amended) The method of claim 16, further comprising blocking ~~communications or~~ packets not associated with the filtering rules associated with the new application.

22. (Currently Amended) The method of claim 16, ~~further comprising inspecting received communications or packets and checking a blocking history to identify~~ wherein the one or more questionable packets include ~~communications or packet types which are defined as those communications/packet~~ packets or packet types ~~observed during the time window to be associated with the application but which are~~ already included in the firewall policy or ~~communications/packet types~~ which were previously blocked at times other than during the time window but which are now observed during the time window.

23. (Currently Amended) The method of claim 16, further comprising ~~modifying the firewall policy rules formed for the new application to provide for blocking the questionable communications or packets~~ determining whether the request to modify the firewall policy is a first attempt, wherein if the new application is determined to include one or more questionable packets and the request to modify the firewall policy is a first attempt, the at least a portion of the packets associated with the new application does not include the one or more questionable packets.

24. (Currently Amended) The method of claim 16, further comprising if the new application is determined to include one or more questionable packets, recording the one or more questionable ~~communications or packet types~~ packets in a blocking history database.

25. (Currently Amended) The method of claim 16, further comprising sending an acknowledgement to ~~the~~ a user's processing device to repeat an attempt to modify the firewall policy when the new application does not function properly through the network-based firewall after the firewall policy has been modified.

26. (Currently Amended) The method of claim 16, further comprising notifying ~~the~~ a user's processing device after a configurable number of repeat attempts ~~that~~ fail to modify the firewall policy such the new application can function properly through the firewall.

27. (Currently Amended) The method of ~~claim 16~~ claim 23, ~~further comprising allowing communications or packets associated with the new application to pass through the network-based firewall~~ wherein if the new application is determined to include one or more questionable packets and the request to modify the firewall policy is not associated with a first attempt, the at least a portion of the packets associated with the new application includes at least a portion of the one or more questionable packets.

28. (Currently Amended) The method of ~~claim 22~~ claim 16, ~~wherein the examining step further comprises~~ further comprising if the new application is determined to include one or more questionable packet, grouping the one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets ~~types of questionable packets singly and in combination of two or more~~.

29. (Currently Amended) The method of claim 28, ~~wherein the examining step~~ further ~~comprises~~ comprising prioritizing the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function ~~properly,~~ properly; and labeling the groups in order of priority.

30. (Currently Amended) The method of ~~claim 28~~ claim 29, ~~wherein examining step~~ further comprising performing successive policy modification attempts to remove ~~previously added~~ one or more of the questionable packet groups previously included in the portion of the packets associated with the new application and ~~adding~~ to add one or more of the ~~next highest priority~~ questionable packet groups having a next highest priority to the portion of the packets associated with the new application ~~firewall policy~~.

31. (Currently Amended) A computer-readable medium for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

logic configured to ~~notify a coordinating entity of~~ receive a request to modify a firewall policy to incorporate filtering rules to allow ~~communications or~~ packets ~~from~~ associated with a new application to pass through the ~~network-based~~ firewall without being blocked;

~~logic configured to notify a policy modifier of the modification request;~~

logic configured to send a user an indication of a time ~~period~~ window during which the user can exercise ~~a new~~ the new application; ~~and~~

logic configured to examine the ~~communications or~~ packets traversing to/from the ~~network-based~~ firewall from/to the user to determine whether the new application includes one or more questionable packets; and

logic configured to ~~modifying~~ modify the ~~user's~~ firewall policy ~~such that necessary communications or packets associated with the new application are allowed~~ to allow at least a portion of the packets associated with the new application to pass through the ~~network-based~~ firewall unblocked, the at least a portion of the packets associated with the new application determined based on whether the new application includes one or more questionable packets.

32. (Original) The computer-readable medium of claim 31, further comprising logic configured to acknowledge the modification request and logic configured to send an acknowledgement of the modification request to a user's processing device.

33. (Original) The computer-readable medium of claim 31, further comprising logic configured to authenticate the user before acting on the modification request.

34. (Currently Amended) The computer-readable medium of claim 31, ~~wherein the logic configured to notify a coordinating entity and~~ further comprising logic configured to notify a policy modifier of ~~a request~~ the request to modify ~~a firewall~~ the firewall policy, ~~is further includes~~ the logic configured to notify the policy modifier further configured to provide a name of the new application and a time frame for ~~implementation of configuration change~~ modifying the firewall policy.

35. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to send an acknowledgement of completion of the modification to ~~firewall facilitation coordinator and to the~~ a user's processing device.

36. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to block ~~communications or~~ packets not associated with the filtering rules associated with the new application.

37. (Currently Amended) The computer-readable medium of claim 31, ~~further comprising logic configured to inspect received packets and logic configured to check blocking history to identify~~ wherein the one or more questionable packets include ~~communications or packet types which are defined as those communications or~~ packets or packet types already included in the firewall policy or ~~communications or packet types~~ which were previously blocked at times other than during the time window but which are now observed during the time window.

38. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to ~~modify the firewall policy rules formed for the new application to provide for blocking previously blocked communications or packets~~ determine whether the request to modify the firewall policy is a first attempt, wherein if the new application is determined to include one or more questionable packets and the request to modify the firewall policy is a first attempt, the at least a portion of the packets associated with the new application does not include the one or more questionable packets.

39. (Currently Amended) The computer-readable medium of ~~claim 31~~ claim 38, ~~further comprising logic configured to inspect received communications or packets and to check a blocking history to identify questionable communications or packet types which are defined as those communications/packet types observed during the time window to be associated with the application but which are already included in the firewall policy or communications/packet types which were previously blocked at times other than during the time window but which are now observed during the time window~~ wherein if the new application is determined to include one or more questionable packets and the request to modify the firewall policy is not associated with a first attempt, the at least a portion of the packets associated with the new application includes at least a portion of the one or more questionable packets.

40. (Canceled)

41. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to record the one or more questionable ~~communications or packet types~~ packets in a blocking history database if the new application is determined to include one or more questionable packets.

42. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to send an acknowledgement to ~~the~~ a user's processing device to repeat an attempt to modify the firewall policy when the new application does not function properly through the ~~network-based~~ firewall after the firewall policy has been modified.

43. (Currently Amended) The computer-readable medium of claim 31, further comprising logic configured to notify ~~the~~ a user's processing device after a configurable number of repeat attempts ~~that~~ fail to modify the firewall policy such that the new application functions properly through the ~~network-based~~ firewall.

44. (Canceled)

45. (Currently Amended) The computer-readable medium of ~~claim 37~~ claim 31, further comprising logic configured to group the ~~types of questionable packets singly and in combination of two or more~~ the one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets if the new application is determined to include one or more questionable packets.

46. (Original) The computer-readable medium of claim 45, further comprising logic configured to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

47. (Currently Amended) The computer-readable medium of ~~claim 45~~ claim 46, further comprising logic configured to perform successive policy modification attempts to remove ~~previously added~~ one or more of the questionable packet groups previously included in the portion of the packets associated with the new application and to add one or more of the ~~next highest priority group~~ questionable packet groups having a next highest priority to the ~~firewall policy~~ portion of the packets associated with the new application.

48. (New) A system for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

a firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy, and to generate a time window during which a user can run the application;

a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation coordinator, to be aware of communications or packets observed by the firewall during the time window, and to modify the user's firewall policy; and

a blocking history checker for checking the communications or packets observed during the time window to be associated with the application in order to identify questionable communications or packets which are defined as those communications/packets or communications/packet types that are already part of the user's firewall policy or

communications or packets previously blocked at times other than during the time window but which are now observed during the time window,

wherein the policy modification agent is further configured to group the types of questionable packets singly and in combination of two or more, and to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

49. (New) The system of claim 48, wherein the policy modification agent is further configured to perform successive policy modification attempts to remove previously added questionable packet groups and to add the next highest priority group to the firewall policy.

50. (New) A method for modifying a firewall policy of a network-based firewall, comprising:

notifying a coordinating entity of a request to modify the firewall policy to incorporate filtering rules to allow communications or packets from a new application to pass through the network-based firewall without being blocked;

notifying a policy modifier of the modification request;

sending a user an indication of a time window during which the user can exercise the new application;

examining the communications or packets traversing to/from the network-based firewall from/to the user and modifying the user's firewall policy such that necessary communications or packets associated with the new application are allowed to pass through the network-based firewall; and

inspecting received communications or packets and checking a blocking history to identify questionable communications or packet types which are defined as those communications/packet types observed during the time window to be associated with the application but which are already included in the firewall policy or communications/packet types which were previously blocked at times other than during the time window but which are now observed during the time window,

wherein examining the communications or packets further comprises grouping the types of questionable packets singly and in combination of two or more, and

wherein examining the communications or packets further comprises prioritizing the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and labeling the groups in order of priority.

51. (New) The method of claim 50, wherein examining the communications or packets further comprises performing successive policy modification attempts to remove previously added questionable packet groups and adding the next highest priority group to the firewall policy.

52. (New) A computer-readable medium for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

logic configured to notify a coordinating entity of a request to modify a firewall policy to incorporate filtering rules to allow communications or packets from a new application to pass through the network-based firewall without being blocked;

logic configured to notify a policy modifier of the modification request;

logic configured to send a user an indication of a time window during which the user can exercise the new application;

logic configured to examine the communications or packets traversing to/from the firewall from/to the user and modifying the user's firewall policy such that necessary communications or packets associated with the new application are allowed to pass through the firewall;

logic configured to inspect received packets;

logic configured to check blocking history to identify questionable communications or packet types which are defined as those communications or packet types already included in the firewall policy or communications or packet types which were previously blocked at times other than during the time window but which are now observed during the time window;

logic configured to group the types of questionable packets singly and in combination of two or more; and

logic configured to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

53. (New) The computer-readable medium of claim 52, further comprising logic configured to perform successive policy modification attempts to remove previously added questionable packet groups and to add the next highest priority group to the firewall policy.